# 基于 SDR 平台的噪声聚合物理层安全传输方案的设计与实现 *

秦鹏翔[1,2]，任品毅[1,2]，杜清河[1,2]，孙　黎[1,2]

(1. 西安交通大学 电子与信息工程学院，西安 710049; 2. 陕西省智慧网络与泛在互联工程技术研究中心，西安 710049)

**摘　要：**噪声聚合物理层安全方案通过编码设计，结合反馈控制可以充分地挖掘无线链路中引入的固有噪声资源，恶化窃听者的信道质量，增强通信系统的安全性能。为了在实际系统中验证与评估该方案的性能，基于软件无线电平台设计并实现了融合噪声聚合抗窃听功能的发射机、接收机方案；在此基础上，搭建了包含源节点、目的节点与窃听节点的抗窃听测试环境。以图像传输业务为测试案例，对误帧率、峰值信噪比等客观指标以及图像主观效果进行了评估。测试结果表明，合法接收端相比于窃听端在同一误帧率条件下可获得良好的信噪比增益；在同一信噪比条件下具有高峰值信噪比且清晰可辨的接收图像，验证了噪声聚合方案的有效性。

**关键词：**软件无线电；无线物理层安全；噪声聚合；图像传输

**中图分类号：**TN915.08　　doi: 10.19734/j.issn.1001-3695.2018.08.0555

# Design and implementation of noise aggregation scheme in physical layer security based on software defined radio

Qin Pengxiang[1,2], Ren Pinyi[1,2], Du Qinghe[1,2], Sun Li[1,2]

(1. *School of Electronics & Information Engineering, Xi'an Jiaotong University, Xi'an* 710049, *China*; 2. *Shaanxi Intelligent Network & Ubiquitous Interconnection Engineering Technology Research Center, Xi'an* 710049, *China*)

**Abstract:** With feedback control method, the physical layer security scheme via noise aggregation can degrade the eavesdropper's channel quality and enhance the security performance of communication system by fully extracting the resources of inherent noise in wireless communication. In order to validate and evaluate the performance of the scheme, this paper designed and realized a practical scheme for transmitter and receiver with anti-wiretapping functions based on software defined radio platform. On basis of that, this paper established the anti-wiretapping test environment, which includes a source node, a destination node and an eavesdropper node. Taking the test case of image transmission, this paper evaluated some objective indicators, such as frame error, peak signal noise rate and the subjective quality of images. Test results show that there is satisfied SNR gain between Bob and Eve for the same frame error rate. Moreover, clear and recognized received images with higher peak signal noise rate prove the effectiveness of the noise aggregation scheme.

**Key words:** software defined radio; wireless physical layer security; noise aggregation; image transmission

## 0　引言

随着无线通信技术的持续革新，多样化的移动业务融入了人们的生活。然而，无线传播环境的固有开放特性使通信系统始终面临着数据易被窃取、隐私难于保护等安全威胁[1]。基于密码学理论，传统的安全机制通过对数据进行秘钥加密来确保信息的安全传输。它的基本思想是使得窃听者破解信息时需要极高的计算复杂度，致使无法破解信息或者破解时间过长从而失去信息的时效性。然而，近年来高性能芯片正在快速发展，传统以计算复杂度为基础的加密机制面临巨大挑战。

物理层安全技术[2]则从另一角度去探索无线通信中的安全传输。不同于传统安全机制，物理层安全基于香农信息论，利用无线信道的物理特征，在不依赖于计算复杂度的情况下可以恶化窃听者信道质量，以此来增强安全。贺洪亮等人[3,4]结合网络编码与 ARQ 反馈关联数据包来增强文件的传输安全并研究了噪声反馈对提高物理层安全性能的关键作用。徐洪斌等人[5,6]基于双向协作系统提出了星座旋转辅助方法与星座重叠方法来防止不可信中继对保密信息进行解码。丁志国等人[7]研究了天线选择对系统安全性能的影响。

噪声聚合[8]物理层安全方案是近几年才被提出的新型物理层安全技术，其可以利用无线链路中固有噪声从而恶化窃听者的信道质量。配合反馈重传机制，可保证合法接收者可靠传输的同时，使窃听者解密极少甚至无法解密保密信息，从而实现安全传输。噪声聚合物理层安全方案利用了通常被认为有害的固有噪声，不需要引入人工噪声；仅仅配合反馈重传机制即可保证安全，实现简单且保密效果好；与大部分物理层安全技术相结合，可以进一步提高安全等级。

当前关于噪声聚合物理层安全方案的研究还处在理论分析和仿真评估阶段。文献[8]阐述了噪声聚合物理层安全方案

**收稿日期：**2018-08-23；**修回日期：**2018-09-29　**基金项目：**陕西省重点研发计划资助项目（2017ZDXM-GY-012）；国家自然科学基金资助项目（61431011）

**作者简介：**秦鹏翔（1994-），男，陕西兴平人，硕士研究生，主要研究方向为软件无线电、无线物理层安全（qinpengxiang@stu.xjtu.edu.cn）；任品毅（1971-），男，湖南长沙人，教授，博导，主要研究方向为认知无线电网络、MIMO 系统、无线通信中的博弈论、无线中继、路由、物理层安全；杜清河（1979-），男，陕西西安人，副教授，博导，主要研究方向为无线移动通信与网络中的跨层设计、5G 网络、移动多播、认知无线电网络、物理层安全；孙黎（1983-），男，陕西西安人，副教授，博导，主要研究方向为无线移动通信与网络中的中继、物理层安全、5G 网络.

原理，并仿真对比了应用噪声聚合方案时不同信道质量下合法接收者与窃听者的误码率、误帧率等指标。文献[9]分析了应用噪声聚合方案时二进制对称信道下合法接收者与窃听者的平均私密速率。截止目前，相关研究均未从实际系统中验证与评估噪声聚合物理层安全方案，现实意义较小。

基于以上思想和前人所做的研究工作，本文利用 NI 公司的通用软件无线电[10]外设（USRP-RIO）设计并搭建了面向噪声聚合安全方案的通信系统。以图像传输业务为例，测试并验证了噪声聚合物理层安全方案的有效性。

## 1　系统模型

面向噪声聚合的系统模型如图 1 所示，其中包含单个源节点 Alice、单个目的节点 Bob 和单个窃听节点 Eve。相比于 Wire-tap 模型[11]，该网络除了存在合法链路外，在 Bob 与 Alice 之间还存在一条反馈链路。在 Eve 存在的情况下，Alice 需要向 Bob 传输保密信息。

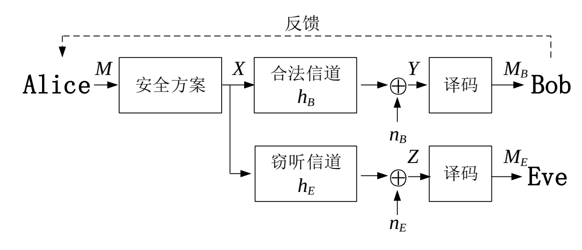



图 1　面向噪声聚合的系统模型

Fig. 1　System model for noise aggregation

图 1 中，$M$ 表示需要发送的保密信息，经过安全方案处理后变为待传输信息 $X$；$h_B$ 与 $h_E$ 分别表示合法信道与窃听信道的信道增益；$n_B$ 与 $n_E$ 分别表示 Bob 与 Eve 接收端噪声；$Y$ 与 $Z$ 表示 Bob 与 Eve 的接收信息；$M_B$ 与 $M_E$ 分别表示 Bob 与 Eve 恢复的保密信息。

当 Alice 向 Bob 传输保密信息时，由于无线传播环境的开放性，Alice 发出的信号不仅经过合法信道被 Bob 所接收，也经过窃听信道被 Eve 所接收。假设 Bob 与 Eve 的接收机完全相同，合法信道与窃听信道均为准静态衰落信道且相互独立。由于 Bob 与 Alice 之间存在反馈链路，当 Bob 发生丢帧时，其可以通过反馈及时告知 Alice 并要求重传丢帧。但 Eve 与 Alice 之间没有反馈链路，当 Bob 收到正确帧后，Eve 有可能仍未正确接收该帧。此时，Eve 将永远失去其包含的保密信息，导致 Eve 无法完整接收，从而实现了安全传输。

在上述系统模型中，若没有安全方案，则 Bob 相比于 Eve 仅仅存在反馈的优势。在此基础上，当合法信道质量与窃听信道质量相当且误帧率均接近于 1 时，Bob 正确接收一帧后 Eve 仍未正确接收该帧的概率仅为 50%。此时，Eve 大致可以正确接收一半的保密信息，保密效果差。

## 2　噪声聚合方案原理

噪声聚合方案可以利用信道中的固有噪声恶化信道质量。配合反馈机制，大大提高 Bob 正确接收一帧后 Eve 仍未正确接收该帧的概率，使 Eve 接收到的有效信息极少甚至为零，从而保证信息安全。现已被提出的噪声聚合方案原理如图 2 所示。

以错误概率为 $\varepsilon_i$ 的二进制对称信道为例。原始帧 $X_1,X_2,\ldots,X_n$ 由等长分组的预发送的比特数据形成。在发送第奇数帧 $X_{2t-1}$ 时，直接发送 $X_{2t-1}$；当发送偶数帧 $X_{2t}$ 时，则发送该偶数帧与上一个奇数帧的异或，即 $X_{2t-1}\oplus X_{2t}$。$W_i$ 为接收第 $i$ 个帧时伴随的噪声。

噪声聚合方案使偶数帧需要与上一个奇数帧共同解包。若 Eve 丢失了一个偶数帧，则无法解密其包含的信息。即使 Eve 正确接收到了偶数帧，但丢失了上一个奇数帧，也无法解密。由此看出，噪声聚合方案增大了偶数帧的丢帧率，等效恶化了偶数帧信道。虽然 Bob 与 Eve 的偶数帧信道同时收到了恶化，但是 Bob 与 Alice 间存在反馈链路，可以通过反馈协议进行可靠传输。

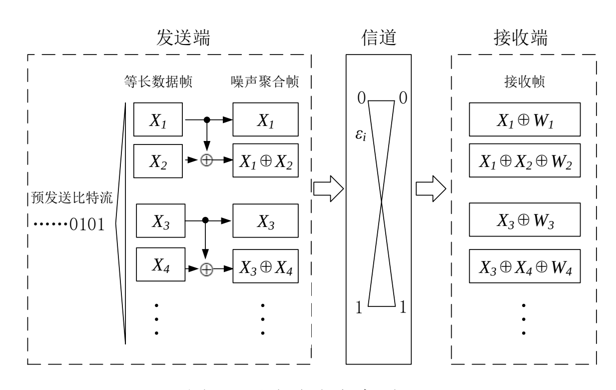



图 2　噪声聚合方案原理

Fig. 2　Principles of noise aggregation

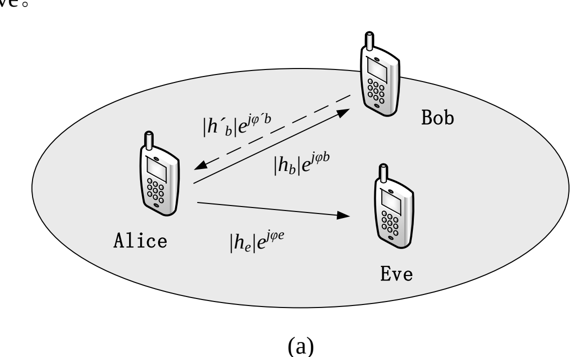
## 3　噪声聚合技术验证系统设计与实现

### 3.1　验证系统概述

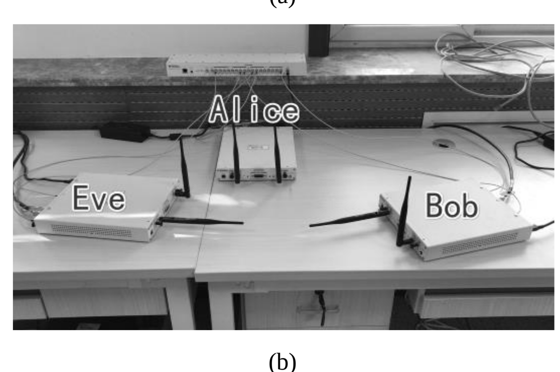
本文利用 USRP-RIO 设备，根据上文中的系统模型以及噪声聚合方案原理，设计并搭建面向噪声聚合的无线通信系统与测试场景。

测试方案的网络拓扑结构如图 3（a）所示，测试场景如图 3（b）所示。图 3（a）中 $|h_b|e^{j\varphi_b}$、$|h_e|e^{j\varphi_e}$、$|h_b'|e^{j\varphi_b'}$ 分别表示合法传输信道、窃听信道以及反馈信道的信道增益。

系统中硬件部分主要由三台 PC 机、三台 USRP-RIO 设备与一个外接时钟源构成。三台设备分别代表 Alice、Bob 和 Eve。




(a)




(b)

图 3　测试方案的网络拓扑与测试场景

Fig. 3　Network topology and testing scenario for noise aggregation

USRP-RIO 设备以射频电路为主，实现无线信号收发、混频、数模或模数转换、数字上下变频等处理。三台设备采用同一个外接时钟源并各自通过一根 PCIe 总线分别与一台 PC 机连接进行高速数据传输，实现无线信号的实时采集与基带处理。软件部分对基带数字采样信号进行处理，采用 Windows 平台下的 Labview 与 Matlab 软件。此外，Labview 通过.VI 文件的前面板实现了人机交互。在 Labview 中调用 Matlab 脚本并编写代码，可以实现噪声聚合物理层安全方案以及其他基带数据处理；利用 Labview 多线程并行、模块化的特点，编辑.VI 文件中的程序框图可以同时进行组帧与解帧，进而实现节点间实时的数据传输或反馈。

### 3.2　链路与帧结构设计

根据对应用场景以功能需求的分析，面向噪声聚合的数字通信链路与帧结构设计如图 4 所示。

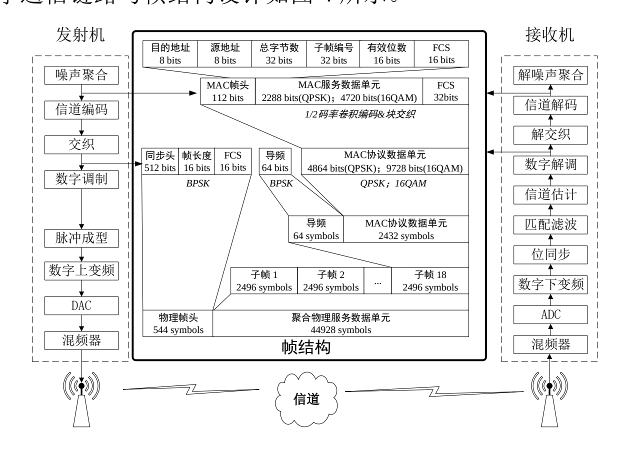



图 4　面向噪声聚合的数字通信链路与帧结构

Fig. 4　Digital communication link and frame structure for noise aggregation

### 3.3　发射机设计

面向噪声聚合方案的发射机由基带部分与上变频部分组成。基带部分包括噪声聚合、信道编码、交织、数字调制、脉冲成型滤波，实现对数据的基带处理。上变频部分包括数字上变频、DAC（digital to analog converter，数模转换器）与混频器，实现对数据的上变频处理。比特数据经过基带处理与上变频处理后转变为无线射频信号，通过无线发送出去。

#### 3.3.1 帧结构设计

链路的帧结构参考 802.11 标准。根据 802.11n 中的帧聚合机制[12]，链路采用改进后的 A-MPDU（MPDU aggregation）帧作为物理帧结构，如图 4 所示。

考虑到实际场景中信道的时延扩展、时变性以及通信系统的基带速率，设计的物理帧由 544 符号长度的物理帧头与 44928 符号长度的聚合物理服务数据单元组成。

物理帧头包含同步头、帧长度以及 FCS（frame check sequence,帧检错序列）。其影响着位同步，故采用 BPSK 调制方式。由于过长的同步头会导致有效数据占物理帧长的比重变小，效率降低，而过短则会降低同步精度，故同步头选取长度适中的 512 位 m 序列。利用 m 序列良好的相关特性可以实现精确的位同步。16 位的帧长度表明了该物理帧包含的有效子帧个数。物理帧头的 FCS 采用 16 位 CRC 校验。

聚合物理服务数据单元由 18 个 2496 符号长度的子帧组成。每个子帧包括 64 符号长度的导频与 2432 符号长度的 MAC 协议数据单元。考虑室内信道相干时间与发射机的基带速率，导频间隔长度即子帧长度应近似为 2500 符号长度。又考虑到导频需满足 01 出现概率相同、长度必须适中等原则，子帧选取 64 位 m 序列作为导频，用作直流偏执消除与信道估计。

MAC 协议数据单元由经过卷积编码和交织的 MAC 帧头、MAC 服务数据单元、FCS 组成。其中，MAC 帧头占 112 位，FCS 占 32 位，MAC 服务数据单元的长度由调制方式决定。若调制方式为 QPSK，MAC 服务数据单元占 2288 位；若调制方式为 16QAM，MAC 服务数据单元占 4720 位。32 位 FCS 采用 CRC 校验，用作对 MAC 服务数据单元检错。

MAC 帧头由 8 位目的地址、8 位源地址、32 位总字节数、32 位子帧编号、16 位有效位数、16 位 FCS 组成。其中，32 位总字节数表示传输文件的总字节大小。16 位有效位数表示该子帧中 MAC 协议数据单元所含有效信息位数。FCS 采用 16 位 CRC 校验，用做对 MAC 帧头检错。

#### 3.3.2 信源数据处理

图像在无线保密通信中是常用的传输对象，通过对比 Bob 和 Eve 的图像质量也能够直观地看出安全方案的保密效果，故选取图像作为数据源。为了防止 Eve 由于图像配置信息丢失而无法显示图像，事先将图像文件拆分为配置信息部分与像素信息部分。测试时，Alice 只传输像素信息部分。Bob 与 Eve 接收完毕后将接收信息与已知的配置信息部分组合生成图像文件。

若 Alice 按图像行顺序发送像素点数据。当 Eve 彻底丢帧时，其只会失去该帧所含的行方向像素点信息。由于失去不相邻行方向信息并不影响整个图像识别，而同时失去相邻行方向信息的概率又极小，故 Alice 按图像行顺序发送无法实现图像保密。按图像列顺序发送像素点数据同理。

为了解决上述问题，在解析图像的像素信息时，将图像分割为合适大小的矩形块，并且对这些块随机排序并组帧发送。若 Eve 发生丢帧，由于每个帧含有许多相邻行列的像素点信息，故 Eve 将丢失该帧包含的图像块信息。此时，Eve 将无法识别图像，达到图像保密效果。

### 3.4　接收机设计

面向噪声聚合方案的接收机由下变频部分与基带部分组成。下变频部分包括混频器、ADC（analog to digital converter，模数转换器）与数字下变频，实现对数据的下变频处理。基带部分包括位同步、匹配滤波、信道估计、数字解调、解交织、信道解码与解噪声聚合，实现对数据的基带处理。无线射频信号被天线接收，经过下变频处理与基带处理后转变为比特数据。Eve 与 Bob 接收机相同，但没有发射机。

#### 3.4.1 直流偏执消除

实验设备 USRP-RIO 为直接变频接收机[13]，即零中频接收机。与超外差接收机不同，其本振频率与载波频率近似相同，虽然简化了接收机结构，却引入了额外的直流偏执。

位同步需要选取相关峰值，而直流偏执的存在会导致相关后序列出现“假峰值”的情况。不仅如此，直流偏执还会改变判决量与标准星座点的欧氏距离，从而影响符号判决。如果不消除直流偏执，位同步以及符号判决等操作均无法正常进行。

Hanning 窗可使大多数交流能量从直流区间中分离，从而消除位同步时出现的“假峰值”。但是 Hanning 窗会将基带信号在零频处的冲激同时消除，故仅利用此方法辅助实现位同步。位同步完成后，未经过 Hanning 窗的基带信号匹配滤波后如下：

$$\begin{aligned} y_k &= (\sqrt{S}Hm_k + \sqrt{N}Z_k + C_k) * h_{-k}^* \\ &= \sqrt{S}H\sum_l h_l m_{k-l} + \sqrt{N}\sum_l h_l Z_{k-l} + C_k\sum_l h_l \end{aligned} \tag{1}$$

其中：$\sqrt{S}$ 为发送与接收的联合增益，$H$ 为信道系数，$m_k$ 为发送波形采样，$N$ 为噪声方差，$Z_k$ 为噪声，$C_k$ 为直流分量，$h_{-k}^{*}$ 为匹配滤波器的单位脉冲响应。

$y_k$ 在最高信噪比 $nN_{ss}$ 时刻采样后的 $y_n$ 如下:

$$y_n = y_k \mid_{k=nN_{ss}} = \sqrt{S} H a_n + \sqrt{N} w_n + C_k \sum_l h_l \tag{2}$$

其中：$w_n = \sum_l h_l Z_{k-l} \mid_{k=nNss}$ 为噪声采样，$a_n$ 为发送符号。根据 m 序列 0 与 1 数量相同的特征、导频为 BPSK 调制、$w_n$ 为 0 均值的高斯白噪声可知，$y_n$ 取均值后只会留下 $C_k \sum_l h_l$ 一项。消去 $C_k \sum_l h_l$ 项即达到消除直流分量的目的，而且不会损失基带信号在零频率处的冲激信息。

### 3.4.2 反馈协议设计

上文的系统模型中，反馈链路是 Bob 区别于 Eve 的重要方面，它保证了 Bob 的可靠传输。反馈链路需要反馈协议的支持，而反馈协议的选择会影响 Eve 的接收效果，进而影响系统的保密性能。目前，实际通信系统中的反馈协议大多采用 ARQ（automatic repeat request, 自动重传请求）协议。常用的 ARQ 协议有停止等待 ARQ 协议，连续 ARQ 协议以及选择性重传 ARQ 协议。

若采用停止等待 ARQ 协议，发送端会不断重传一帧直到收到该帧对应的 ACK（ACKnowledgement，确认）帧。但在信道质量不好时，发送端会长时间重传相同帧，导致传输效率过低。

若采用连续 ARQ 协议，由于存在滑动窗口，发送端可以在未收到 ACK 帧的情况下继续发送下一帧。但在信道质量不好时，会出现 Go-back-N 情况。此时，Aliec 会重传 Bob 已正确接收的帧，导致 Eve 有更大概率接收正确帧从而降低系统保密性能。

若采用选择性重传 ARQ 协议，发送端可以不用等待接收端的应答，并持续发送多个帧，且只重传丢失帧。相比于停止等待 ARQ 协议，传输效率大大提高；相比于连续 ARQ 协议，不会因为 Go-back-N 而重传 Bob 已正确接收的帧。

## 4　实验评估与性能测试

### 4.1　实验参数

在实际的无线通信系统中，Alice 与 Bob 之间为频分半双工通信，单载波调制，传输频段为 5GHz，反馈频段为 2.4GHz。由于 Eve 没有发射机，Eve 只能在传输频段上被动窃听信息。无线数字通信链路的指标参数如表 1、2 所示。

表 1　数字通信链路指标与方法

Table 1　Indicators and methods in digital communication link

| 指标 | 方法 |
|---|---|
| 信道编码 | 1/2 卷积编码 |
| 交织编码 | 块交织 |
| 数字调制 | QPSK；16QAM |
| 脉冲成型(匹配)滤波器 | 根升余弦滤波器 |
| 位同步 | 最大似然时延估计[14] |
| 相关峰值阈值设置 | 均值法[15] |
| 信道估计 | 迫零估计 |
| 判决方式 | 最大似然判决 |
| 信道解码 | 维特比译码 |

表 2　数字通信链路参数与参数值

Table 2　Parameters and corresponding values in digital communication link

| 参数 | 参数值 |
|---|---|
| 卷积编码八进制生成矩阵 | [133,171] |
| 块交织深度 | 24 |
| 根升余弦滤波器相关符号长度 | 100 |
| 根升余弦滤波器滚降系数 | 0.25 |
| 基带速率 | 100kHz |
| 发射机过采样速率 | 300ksps |
| 接收机过采样速率 | 1Msps |

其中由于信道编码采用 1/2 码率的卷积编码，且物理帧包含帧头、导频等冗余信息。故实际中，QPSK 调制方式下的传输速率大约为 10kBps；16QAM 调制方式下的传输速率大约为 20kBps。

### 4.2　观测界面

由于 Alice、Bob、Eve 实现的功能不同，各节点的人机交互界面略有差异但大致相同。以 Eve 节点为例，基于 Labview 的人机交互界面如图 5 所示。人机交互界面主要分为射频配置、基带配置、实时观测三部分。

在射频配置模块中，用户可以轻松配置收发天线口、过采样频率、发送或接收增益、生成或捕获方式、过采样速率等参数。

在基带配置模块中，用户可以对子帧个数、子帧长度、数字调制方式、脉冲成型滤波器相关符号数与滚降系数、接收序列长度、基带速率等参数进行设置。

在实时观测模块中，用户可以实时观测到接收信号的基带波形、功率谱、功率电平以及文件的实时接收进度、当前丢帧号、平均接收功率等信息。在接收完毕后，还可以读取到接收图像相比于原图的峰值信噪比、误帧率等指标。

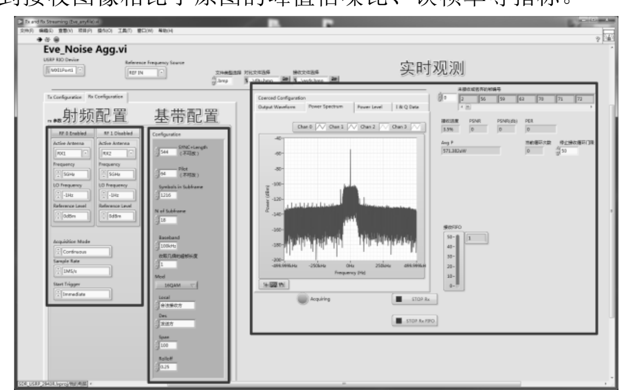



图 5　基于 Labview 的人机交互界面（Eve）

Fig. 5　Interactive interface at Eve based on Labview

除了上述的主要模块外，人机交互界面还包括时钟源选择、发送文件选择、接收地址选择、对比文件选择等部分。

### 4.3　测试结果

由于三台 USRP-RIO 设备相同，故 Bob 与 Eve 的噪声方差可认为近似相同，此时的平均接收信噪比只由平均接收功率决定。通过调整 Bob 与 Eve 的平均接收功率，就可以保证两者平均接收信噪比相同。

以图像传输业务为例，实验记录了不同调制方式、不同平均接收功率条件下，Bob 与 Eve 的误帧率，如表 3、表 4 所示。

对比表 3 与 4 可以看出，在 QPSK 与 16QAM 调制方式下、同一误帧率条件下，Bob 总比 Eve 获得良好的平均接收功率增益，窃听者信道遭到了恶化。

表 3　QPSK 调制方式下 Eve 与 Bob 的误帧率

Table 3　Frame error rate at Bob and Eve in QPSK modulation

| 平均接收功率/uW | Bob 的误帧率(1) | 平均接收功率/uW | Eve 的误帧率(1) |
|---|---|---|---|
| 131 | 0.5726 | 136 | 0.6806 |
| 140 | 0.4420 | 145 | 0.4971 |
| 152 | 0.2856 | 149 | 0.4070 |
| 159 | 0.2157 | 162 | 0.2755 |
| 170 | 0.1329 | 170 | 0.2179 |
| 180 | 0.0655 | 178 | 0.1428 |
| 186 | 0.0337 | 185 | 0.0983 |
| 204 | 0.0174 | 202 | 0.0453 |
| 224 | 0.0076 | 226 | 0.0136 |
| 234 | 0.0042 | 237 | 0.0076 |

表 4　16QAM 调制方式下 Eve 与 Bob 的误帧率

Table 4　Frame error rate at Bob and Eve in 16QAM modulation

| 平均接收功率/uW | Bob 的误帧率(1) | 平均接收功率/uW | Eve 的误帧率(1) |
|---|---|---|---|
| 364 | 0.7496 | 347 | 0.8377 |
| 428 | 0.3513 | 419 | 0.5687 |
| 429 | 0.3655 | 435 | 0.4485 |
| 441 | 0.3110 | 452 | 0.4374 |
| 465 | 0.2132 | 457 | 0.3531 |
| 482 | 0.1357 | 492 | 0.2432 |
| 509 | 0.1132 | 506 | 0.1726 |
| 550 | 0.0423 | 543 | 0.1123 |
| 575 | 0.0203 | 556 | 0.0903 |
| 648 | 0.0086 | 633 | 0.0194 |

为了更加直观地体现噪声聚合方案的优势，图 6 展示了 16QAM 调制方式下，Alice 发送图像与 Eve、Bob 在 373uw 平均接收功率大小时的接收图像。



Alice　　Bob



Eve

图 6　Alice 发送图像与 Bob、Eve 接收图像

Fig. 6　Transmitted image at Alice, received images at Bob and Eve

可以看出，在同一平均接收功率条件下，同一信道质量条件下，Eve 的接收图像受到严重污染，完全无法识别图像。但是 Bob 却能恢复出原始图像，实现了保密传输。

图像质量的客观评价与主观评价同样重要。通过计算图像的 PSNR（peak signal to noise ratio，峰值信噪比）可以得出对图像客观的评价，其表现为图像间的相似程度。图像间 PSNR 值越小，则越失真。

由于 Bob 是可靠接收，所以只有 Eve 存在 PSNR 值。实验记录了在不同调制方式、不同平均接收功率条件下，Eve 接收图像与原图相比的 PSNR 值，如表 5 所示。

由表 5 可以看出，在 QPSK 与 16QAM 调制方式下、不同平均接收功率条件下，Eve 接收图像相比于原图的 PSNR 值均低于普遍基准即 30 dB。故可以认为 Eve 的图像较 Bob 劣化明显，证实了噪声聚合方案的有效性。

表 5　Eve 接收图像的峰值信噪比

Table 5　PSNR of received image at Eve

| 平均接收功率/uW | QPSK 调制下 PSNR/dB | 平均接收功率/uW | 16QAM 调制下 PSNR/dB |
|---|---|---|---|
| 131 | 7.16 | 364 | 6.72 |
| 140 | 7.99 | 428 | 7.32 |
| 152 | 7.99 | 429 | 7.85 |
| 159 | 9.03 | 441 | 8.92 |
| 170 | 9.34 | 465 | 8.92 |
| 180 | 10.00 | 482 | 9.54 |
| 186 | 10.41 | 509 | 10.41 |
| 204 | 11.14 | 550 | 11.14 |
| 224 | 12.79 | 575 | 11.14 |
| 234 | 13.98 | 648 | 13.01 |

## 5　结束语

基于软件无线电平台，本文设计了融合噪声聚合抗窃听能力的发射机与接收机方案，并搭建了相应的抗窃听测试环境。以图像传输业务为例，用实测数据验证了噪声聚合物理层方案的保密性能。在现有理论分析及仿真评估的基础上，为噪声聚合方案的有效性提供了现实依据。另外，基于软件无线电的数字通信链路与帧结构设计对于后续完善以及其他物理层安全方案的原型实现提供了参考与借鉴。

## 参考文献：


[1] 沈昌祥，张焕国，冯登国，等. 信息安全综述 [J]. 中国科学：技术科学, 2007, 37(2): 129-150. (Shen Changxiang, Zhang Huanguo, Feng Dengguo, *et al.* Summary of information safety [J]. Scientia Sinica: Technologica , 2007, 37(2): 129-150. )

[2] Bloch M, Barros J. Physical-layer security: from information theory to security engineering [M]. Cambridge: Cambridge University Press, 2011.

[3] He Hongliang, Ren Pinyi. Secure ARQ protocol for wireless communications: performance analysis and packet coding design [J]. IEEE Trans on Vehicular Technology, 2018, PP(99): 1-1.

[4] He Hongliang, Ren Pinyi, Sun Li, *et al.* Secure communication using noisy feedback [C]//Proc of Global Communications Conference. IEEE, 2016: 1-6.

[5] Xu Hongbin, Sun Li, Ren Pinyi, *et al.* Securing two-way cooperative systems with an untrusted relay: a constellation-rotation aided approach [J]. IEEE Communications Letters, 2015, 19 (12): 2270-2273.

[6] Xu Hongbin, Sun Li, Li Fan. Towards enhanced security for two-way untrusted relaying systems: a constellation overlapping scheme [C]// Proc of IEEE International Conference on Communications. IEEE, 2018: 1-7.

[7] Ding Zhiguo, Ma Zheng, Fan Pingzhi. Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise [J]. IEEE Trans on Wireless Communications, 2014, 13(4): 2189-2203.

[8] Hussain Mukhtar, Du Qinghe, Sun Li, *et al.* Security enhancement for video transmission via noise aggregation in immersive systems [J]. Multimedia Tools & Applications, 2016, 75(9): 5345-5357.

[9] Xu Qian, Ren Pinyi, Du Qinghe, *et al.* On achievable secrecy rate by noise aggregation over wireless fading channels [C]//Proc of IEEE International Conference on Communications. IEEE, 2016: 1-6.

[10] 向新. 软件无线电原理与技术 [M]. 西安: 西安电子科技大学出版社, 2008. (Xiang Xin. Principle and technology of software radio [M]. Xi'an: Xidian University Press, 2008. )

[11] Wyner A D. The wire-tap channel [J]. Bell Labs Technical Journal, 1975, 54 (8): 1355-1387.

[12] 刘维穆, 刘厚泉. 无线局域网 IEEE 802. 11n 标准分析 [J]. 信息通信, 2008, 21(4): 36-39. (Liu Weimu, Liu Houquan. Analysis of WLAN IEEE 802. 11n standard [J]. Information & Communications, 2008, 21(4): 36-39. )

[13] Razabi B. Design Consideration for Direct-Conversion Receivers [J]. IEEE Trans. on Circuits Syst. ii, 1997, 44(6): 428-435.

[14] Forney G. Maximum-likelihood sequence estimation of digital sequences in the presence of intersymbol interference [J]. IEEE Trans on Information Theory, 2003, 18(3): 363-378.

[15] 王森. 基于软件无线电的通信系统设计与实现 [D]. 西安: 西安电子科技大学, 2015. (Wang Sen. Design and implementation of communication system based on Software Radio [D]. Xi'an: Xidian university, 2015. )